Supliment al revistei „Impact strategic”

COLOCVIU STRATEGIC

UNIVERSITATEA NAȚIONALĂ DE APĂRARE „CAROL I”

CENTRUL DE STUDII STRATEGICE DE APĂRARE ŞI SECURITATE

Nr. 10 (177) / 2020
Indexat în
CEEOL și ROAD

DELIMITĂRI CONCEPTUALE PRIVIND OPERAȚIILE INFORMAȚIONALE, CIBERNETICE, NON-LETALE ȘI NON-CINETICE

Alexandru PINTILI
Ion MITULEȚU

Conceptual boundaries on information, cyber, non-lethal and non-kinetic operations

Abstract: *The technological revolution marked the end of the 20th century – the beginning of the 21st century, characterized by the use of electronic tools for large-scale information processing and the freedom of access to the global information space. The achievements of the technological revolution were used to create high-precision weapons, information systems and military equipment, state-of-the-art research in military electronics, etc. They represent the foundation on which the weapons systems of modern armies are built. This resulted in a change in the approach to war, based on accelerated computerization and technological discoveries, which made possible the creation not only of global reconnaissance, communications and navigation systems, but also the interconnection of different weapons, reconnaissance, command and control systems, which led to the achievement of informational and decision-making superiority.*

In this context, developments in the security environment determine the trend of emerging and disruptive technologies, based on artificial intelligence, 5G networks, virtual and information systems, etc. The integration of emerging and disruptive technologies in military operations determines a new type of approach regarding their characteristics and physiognomy. Therefore, there is the development of new concepts related to information, cybernetic, non-lethal and non-kinetic operations. Given this approach, we aim to identify the conceptual boundaries of these types of operations and to assess the extent to which they are integrated and interconnected, depending on the nature of the emerging risks and threats.

Keywords: *information environment, information operations, virtual space, cyber operations, non-lethal operations, non-kinetic operations.*

Delimitări conceptuale privind operațiile informaționale, cibernetice, non-letale și non-cinetice

Rezumat: *Revoluția tehnologică a marcat sfârșitul secolului XX – începutul secolului XXI, aceasta caracterizându-se prin utilizarea instrumentelor electronice de prelucrare a informațiilor la scară largă și prin libertatea de acces la spațiul informațional global. Realizările revoluției tehnologice au fost utilizate pentru crearea armelor de înaltă precizie, sistemelor de informații și echipamente militare, cercetări de ultimă generație în electronica militară etc. Ele re-prezintă fundamentul pe care se construiesc sistemele de armamente ale armatelor moderne. De aici a rezultat și o schimbare în abordarea războiului, bazată pe informatizarea accelerată și descoperirile tehnologice, fapt ce a făcut posibilă crearea nu numai a sistemelor globale de recunoaștere, comunicații și navigație, ci și interconectarea diferitelor sisteme de armament, recunoaștere, comandă și control, ceea ce a dus la obținerea superiorității informaționale și decizionale.*

În acest context, evoluțiile din mediul de securitate determină tendința de dezvoltare a tehnologiilor emergente și disruptive, bazate pe inteligența artificială, rețelele 5G, sistemele virtuale și informaționale, etc. Integrarea tehnologiilor emergente și disruptive în cadrul operațiilor militare determină un nou tip de abordare privind caracteristicile și fizionomia acestora. Astfel, se constată dezvoltarea unor concepte noi referitoare la operațiile informaționale, cibernetice, non-letale și non-cinetice. Având în vedere această abordare, ne propunem să identificăm delimitările conceptuale ale acestor tipuri de operații și să evaluăm în ce măsură sunt integrate și interconectate, în funcție de natura riscurilor și amenințărilor emergente.

Cuvinte-cheie: *mediul informațional, operații informaționale, spațiul virtual, operații cibernetice, operații non-letale, operații non-cinetice.*

Lt. Alexandru PINTILI *este doctorand în domeniul Științe Militare în cadrul Universității Naționale de Apărare „Carol I” din București (e-mail: alexandru.pintili@rdietc.ro, alex.pintili91@gmail.com).*

Col. (r) prof. univ. dr. Ion MITULEȚU *este conducător de doctorat în cadrul Universității Naționale de Apărare „Carol I” din București (e-mail: mituletuion@yahoo.com).*

Operațiile informaționale

Războaiele și operațiile informaționale, importanța lor în politica modernă și în alte domenii ale vieții sunt în prezent subiectul unor discuții ample. Cu toate acestea, uneori există impresia că esența unor astfel de războaie pare să fie interpretată oarecum simplist, ceea ce, la rândul său, face dificilă rezolvarea problemelor complexe de securitate a informațiilor. Între timp, a luat naștere un nou tip de război informațional care necesită o cercetare multilaterală și aprofundată.

Ca un exemplu clasic al unei operații informaționale efectuate în trecutul istoric îndepărtat, este adesea menționat planul de cucerire a cetății Troia dezvoltat și implementat de Odiseu (sec. XII î.Hr.). Acest eveniment pare a fi o operațiune de dezinformare a inamicului, nimic mai mult. Cu toate acestea, o analiză mai detaliată permite descifrarea profunzimii planului și a nivelului ridicat de gândire strategică a grecilor din acele timpuri[1].

Operațiile informaționale, într-o formă sau alta, au fost folosite în aproape toate războaiele omenirii. Conținutul modern și terminologia operațiilor informaționale au început să se contureze începând cu anii ’90. În 1998, era deja adoptată Doctrina operațiilor informaționale ale Departamentului american al Apărării, unde se prezentau definițiile conceptelor de „operație informațională” și „război informațional”:

- operație informațională – acțiuni întreprinse pentru a complica colectarea, procesarea, transmiterea și stocarea informațiilor de către sistemele de informații inamice, protejând în același timp sistemele de informații proprii;
- război informațional – un impact cuprinzător asupra sistemului de administrație al părții adverse și a conducerii sale politico-militară, care, în timp de pace, poate duce la adoptarea deciziilor nefavorabile inamicului, iar în timpul unui conflict armat poate paraliza complet funcționarea infrastructurii administrative a acestuia.[2]

Putem observa că unele caracteristici ale războaielor informaționale seamănă cu „Strategiile” lui Sun Tzu. În prezența unor fluxuri de informații puternice (care creează „haos în mintea societății”) este aproape imposibil să reziști amenințărilor.[3]

Operațiile informaționale reprezintă acțiuni întreprinse pentru a obține superioritatea informațională în fața inamicului prin influențarea sistemelor de informații ale acestuia, în același timp consolidând și protejând propriile sisteme de informații. Într-un sens mai larg, sistemele informaționale sunt reprezentate atât de sistemele tehnice, cât și de sfera psihologică, astfel încât se disting două zone ale operațiilor informaționale: tehnică și psihologică.

Sfera tehnică este zona de spațiu informațional în care informațiile sunt create, procesate și stocate. În plus, acesta este un domeniu în care operează sistemele de comandă, control și comunicare. Dezvoltarea și perfecționarea conceptului de sferă tehnică a spațiului informațional a condus la crearea aparatului conceptual al spațiului cibernetic. Sfera psihologică este zona din spațiul informațional care unește gândirea personalului militar și a civililor. Acesta este un domeniu în care sunt formate intențiile comandantului, doctrinele, tactica, metodele de confruntare, moralitatea, conceptul de coeziune a unității, nivelul de pregătire, experiența, înțelegerea situației și opinia publică.[4]

În funcție de obiectivele și nivelul de management asupra cărora se realizează impactul, operațiile informaționale pot fi clasificate în cele la nivel de stat și cele la nivel militar.[5]

La nivel de stat, obiectivele unei operații informaționale sunt slăbirea pozițiilor statelor concurente, subminarea fundamentelor lor de stat național, încălcarea sistemului de guvernare datorită impactului informațional asupra sferelor politică, diplomatică, economică și socială ale societății, desfășurarea operațiilor informațional-psihologice, subversive și alte acțiuni de propagandă. În plus, acest tip de operații pot rezolva problemele protejării intereselor naționale, prevenirea conflictelor internaționale, reprimarea actelor provocatoare și teroriste, precum și asigurarea securității resurselor naționale.

La nivel militar, operațiile informaționale reprezintă un ansamblu de activități desfășurate în cadrul forțelor armate ale unei țări și fac parte integrantă din operațiile militare. Acestea sunt orientate spre obținerea superiorității informaționale față de inamic și protejarea propriilor sisteme de comandă și control.[6] În funcție de nivelul impactului, acest tip de operații pot fi clasificate în: operații informaționale de nivel strategic, operații informaționale de nivel operațional și operații informaționale de nivel tactic.[7]

[1] M. Cartwright, „Odysseus”, *Ancient History Encyclopedia*, 31 December 2012, URL: https://www.ancient.eu/odysseus, accesat la 08.11.2020

[2] V.N. Baranov, V.V. Lazarev, V.V. Selivanov, *Preconditions and capabilities of development and deployment of special means of combined non-lethal effect*, Proceedings of the 3rd European Symposium on Non-Lethal Weapons, Ettlingen, Germany, 10-12 May 2005.

[3] V.V. Selivanov, D.P. Levin, *Non-lethal weapon role and place in complex security systems*, Proceedings of the 7th European Symposium on Non-Lethal Weapons, Ettlingen, Germany, 3-5 June 2013.

[4] ***, *Joint Publication 3-13.1. - Electronic Warfare*, US Joint Chiefs of Staff, 2007, pp. 14-16.

[5] A.N. Sidorin, V.M. Prishchepov, V.P. Akulenko, *Vooruzhennye sily USA v XXI veke: Voenno-teoreticheskii trud [The U.S. Armed Forces in the XXI Century]*, Progress Publishers, Moscow, 2013.

[6] Ibidem, p. 374.

[7] V. Zhukov, „Взгляды военного руководства США на ведение информационной войны [The views of the US military leadership on information warfare]”, *Зарубежное военное обозрение [Foreign Military Review]*, No. 1, 2001, URL: http://pentagonus.ru/publ/22-1-0-175, accesat la 05.11.2020.

Spațiul cibernetic și operațiile cibernetice

Odată cu dezvoltarea aparatului conceptual al confruntării informaționale, a apărut necesitatea obiectivă de a aloca o parte din terminologia referitoare direct la confruntarea în sfera tehnică a spațiului informațional. În Forțele Armate ale SUA și NATO, o astfel de bază terminologică este introdusă printr-o serie de așa-numite „concepte cibernetice".

Problema securității cibernetice devine din ce în ce mai importantă la nivel internațional și, astfel, apar o serie de dileme în spațiul cibernetic: libertate absolută sau control total, haos sau ordine strictă în politica de rețea etc. Utilizarea ultimelor tehnologii informaționale reprezintă o oportunitate, dar și un pericol pentru societate, de aceea, trebuie acordată atenție locului domeniului cibernetic și al inteligenței artificiale în sistemul de securitate al națiunilor, perspectivelor sistemelor de comunicații, problemelor armelor cibernetice, operațiilor și războiului cibernetic.[8]

Prioritatea ridicată într-o operație cibernetică nu este dată numai de daunele produse inamicului, ci și de protecția propriilor date, astfel încât securitatea cibernetică este o parte integrantă a acestui tip de confruntare. Este o combinație de principii, instrumente și strategii pentru a asigura invulnerabilitatea și protecția mediului cibernetic, anume disponibilitatea, integritatea și confidențialitatea datelor.

Conform standardului de securitate cibernetică ISO/IEC 27032:2012, conceptul de „securitate cibernetică" este definit prin cel de spațiu cibernetic. Securitatea cibernetică este reprezentată de securitatea în spațiul cibernetic. Astfel sunt definite legăturile dintre termenii securitate cibernetică, securitatea rețelei, securitatea aplicațiilor, securitatea internetului și securitatea și infrastructura informațională. Standardul oferă o proiecție a acestor termeni în mediul cibernetic.[9]

O operație cibernetică este formată în general din două mari componente: spionaj și atac. Prima etapă presupune colectarea de date cu ajutorul sistemelor informatice. Atacurile pot fi împărțite în funcție de scopul și obiectivul vizat în: operații de vandalism – postarea unor informații și imagini false pe pagini web în locul informațiilor originale; propaganda – utilizarea propagandei în conținutul paginilor web; furtul de date confidențiale – în urma compromiterii unui server vizat, tot ce este de interes este copiat, iar datele confidențiale pot fi înlocuite; diferite tipuri de atacuri, precum cele de tip DDoS – atac cibernetic destinat perturbării unui sistem informatic; crearea de defecțiuni ale echipamentelor informatice – sunt atacate computerele responsabile de operarea echipamentelor informatice. Un astfel de atac duce la defectarea echipamentului sau la oprirea temporară a acestuia.[10]

Cele mai multe operații cibernetice au ca scop perturbarea funcționării sistemelor informatice responsabile de activitatea infrastructurilor critice (financiare, energetice, industriale, rețele de transport, sistem sanitar etc.), a organizațiilor guvernamentale, creând haos. Prin urmare, sunt afectate sisteme importante de susținere a vieții, precum: sisteme de alimentare cu apă, canalizare, centrale electrice, noduri de energie și alte rețele de comunicare etc. Dependența instituțiilor statului, a întreprinderilor și a cetățenilor de internet a crescut semnificativ. În același timp, războiul cibernetic este o adevărată amenințare pentru securitatea țării, având în vedere că atacurile cibernetice ale unui stat îndreptate împotriva altuia pot provoca daune semnificative economiei țării sau efecte ce pot depăși toate așteptările. La urma urmei, crearea unui virus este mult mai ieftină în comparație cu cumpărarea de armament militar.

În prezent, fiecare proces este controlat de tehnologia informației. Fie că este vorba doar de reglementarea traficului, cea mai mică defecțiune poate cauza probleme grave. Folosirea abundentă a tehnologiei a făcut ca civilizația să fie dependentă, deci, vulnerabilă și, prin urmare, este imposibil să fie prezise consecințele unui atac cibernetic amplu. În aceste condiții, majoritatea statelor dezvoltate sunt preocupate de securitatea sistemelor informaționale și au integrat acest aspect în strategiile naționale de apărare. Internetul a devenit o nouă zonă de război. În SUA, „Cybercom" a fost creat pentru acțiuni ofensive și pentru protecția obiectivelor importante împotriva unor amenințări cibernetice. Rusia, începând cu anul 2014, a investit în „trupe cibernetice", responsabile de securitatea informațiilor. Aproximativ douăzeci de mii de hackeri servesc și China. Pe lângă aceste țări, Iranul, Israelul și țările europene fac investiții importante în zona cibernetică.

Operațiile non-letale

Omenirea a intrat în noul mileniu, civilizația face o tranziție către un stat calitativ nou, deoarece în țările dezvoltate societatea însăși este informațională, în care puterea se bazează pe cunoaștere, iar bogăția principală este informația. În legătură cu schimbările în curs de dezvoltare a societății umane, arsenalul de arme și tehnologii de război se schimbă în consecință. Deși în secolul trecut oamenii, bazându-se pe experiența amară a distrugerii cu succes a propriului fel, și-au dat seama de ne-

[8] V.S. Polikarpov, E.V. Polikarpova, *Войны будущего [The wars of the future]*, Algoritm Publishing House, Moscow, 2015, p. 4.
[9] ***, *ISO/IEC 27032:2012 – Information technology - Security techniques – Guidelines for cybersecurity*, URL: https://www.iso27001security.com/html/27032.html, accesat la 20.11.2020.

[10] ***, *Кибервойны (Cyberwarfare)*, Anti-Malware, URL: https://www.anti-malware.ru/threats/cyberwarfare, accesat la 20.11.2020.

cesitatea abandonării războaielor ca mijloc de soluționare a disputelor, lupta pentru putere și avere nu a dispărut, ci a luat alte forme. Trebuie să recunoaștem că, pur și simplu, nu există niciun motiv pentru un mare optimism în ceea ce privește excluderea războaielor din viața popoarelor lumii. Nu este surprinzător faptul că noi tipuri de arme și tehnologii de război apar deja în arsenalele armate, ca expresie a tendințelor în evoluția sistemelor de armament. Drept urmare, a apărut fenomenul războiului multidimensional, ca unitate a factorilor militari și non-militari, inclusiv a armelor neletale (diplomație, inteligență, ideologie, „soft power" etc.).

În prezent, în fața amenințării terorismului, au apărut alte două amenințări majore, care sunt mult mai susceptibile în următorii 50 de ani: un alt război mondial și pandemiile. O abordare rațională a riscurilor unui război major al viitorului sau al III-lea Război Mondial necesită utilizarea unor factori non-militari. Acești factori se referă la așa-numita „intelligent power", care face posibilă transformarea resurselor (financiare, economice, politice, diplomatice etc.) într-o forță continuă în ceea ce privește obținerea rezultatelor dorite[11] și, de aceea, definirea puterii prin contabilizarea resurselor este adecvată realităților moderne și are un caracter productiv.

În acest sens, ideea dezvoltării așa-numitelor „arme neletale", lansată pentru prima dată în SUA și susținută activ de mulți reprezentanți militari, a ieșit în prim-plan. Un impuls suplimentar pentru dezvoltarea lor a fost dat de prezența unui domeniu larg de utilizare a unor astfel de arme, precum lupta împotriva terorismului, contrabandei și a traficului de persoane. „Dezbaterea despre noi tipuri de arme, așa-numita armă neletală, a început în paralel cu o discuție despre noul rol al SUA în lume, după încheierea Războiului Rece. În dezvoltarea ideii creării de noi tipuri de arme (inclusiv a celor legate de tehnologiile informațional-psihologice), s-a sugerat că această armă va schimba conceptul operațiilor militare moderne, iar crearea și utilizarea acesteia va deveni parte a tranziției de la războaiele din epoca industrială cu distrugerea inamicului prin „foc și sabie" spre „războaiele epocii informaționale", unde accentul va fi pus pe „paralizarea" inamicului fără a-l distruge".[12] Armele neletale sunt destinate creării unei situații operaționale favorabile pentru diferite operații militare, de ordine publică, antiteroriste etc. și sunt concepute pentru a învinge partea adversă, dar nu prin distrugerea fizică, ci privarea temporară și reversibilă a capacității de luptă.

Conform Directivei 3000.03E, Departamentul Apărării al SUA definește armele neletale ca „arme, dispozitive și muniții care sunt proiectate și utilizate pentru a incapacita persoanele sau tehnica vizată, în timp ce reduce la minimum decesele, vătămarea personalului și deteriorarea nedorită a proprietăților din zona sau mediul țintă. Armele neletale sunt destinate să aibă efecte reversibile asupra personalului și tehnicii".[13] În viziunea NATO, „armele cu acțiune neletală reprezintă un tip de armament care este dezvoltat și aplicat pentru a distruge personalul și echipamentele militare cu o probabilitate foarte scăzută de deces sau daune iremediabile sănătății și un impact minim nedorit asupra mediului".[14]

Trebuie menționat că armele neletale, destinate utilizării în operații militare limitate, sunt dezvoltate pe baza realizărilor științei moderne și a ultimelor tehnologii. Ele pot include dispozitive care afectează auzul și care provoacă perturbări temporare în coordonare, vărsături și indigestie. Generatoarele de sunete create care afectează psihicul uman sunt, de asemenea, în atenție. Acest tip de generator este un dispozitiv destul de compact care are două microfoane, dintre care unul emite un sunet invizibil care poartă o imagine acustică predeterminată, iar celălalt emite pur și simplu un sunet nemodulat. Ca urmare a impactului acestui generator de sunet asupra subconștientului uman, acesta din urmă se comportă în conformitate cu imaginea acustică codificată. Evident, cu ajutorul mirosurilor și sunetelor ca mijloc de armă neletală, este posibilă, de exemplu, eliminarea lunetiștilor din clădirile vizate și chiar pentru crearea anumitor zone nefavorabile acțiunilor trupelor inamice.[15]

Chiar și termenul de „armă neletală" nu reflectă cu exactitate natura impactului său și consecințele utilizării sale, deoarece unele arme din acest domeniu provoacă boli în masă ale oamenilor și animalelor (adesea fatale), leziuni ireversibile ale ochilor și organelor interne, ceea ce duce la handicap, distrugerea vegetației și a terenului și poate avea efecte pe termen lung. Totuși, complexitatea problemelor prezentate anterior împiedică dezvoltarea rapidă a armelor neletale.

Un punct forte al operațiilor non-letale îl constituie armele electromagnetice. În prezent există o serie de astfel de arme, precum:

- o armă cu impuls – un fel de electroșoc, care permite distrugerea echipamentului sau imobiliza-

---

[11] J.S. Nye, Jr., *Viitorul puterii*, Editura Polirom, Iași, 2012, p. 36.

[12] N.V. Danilov, *Компьютерные технологии как оружие информационно-психологического действия [Computer technologies as a weapon of information and psychological action]*, Proceedings of „The Information Security of Russia" Conference, Moscow, 1998, p. 159.

[13] ***, *Directive 3000.03E: DoD Executive Agent for Non-Lethal Weapons (NLW), and NLW Policy*, U.S. Department of Defense, 25 April 2013, p. 12, URL: http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/300003p.pdf?ver=2018-10-24-112944-467, accesat la 21.11.2020.

[14] ***, *Non-Lethal Weapons and Future Peace Enforcement Operations*, RTO Techical Report TR-SAS-040, NATO, November 2004, p. 1.

[15] S. Samsonov, „Как воспринимаются запахи [How odors are perceived]", *Наука и жизнь ["Science and Life" Journal]*, No. 4, 1988, pp. 161-162.

rea unei persoane cu ajutorul unui șoc electric utilizat de la distanță;

- fulger artificial – este un tip de armă electromagnetică de sabotaj care vizează liniile electrice, radare, dispozitive ale sistemelor de telecomunicații și alte echipamente radio;
- muniție electromagnetică amplasată pe rachete și bombardiere de croazieră utilizate pentru dezactivarea echipamentelor electronice;
- arme cu frecvență radio (cu microunde, ce includ unde radio cu lungimi de undă de milimetru, centimetru și decimetru).[16]

Un alt tip de operație non-letală sunt acțiunile psihologice, ce au ca scop lovirea soldaților inamici chiar și înainte ca aceștia să îmbrace uniforma militară, atunci când sunt deosebit de vulnerabili în mediul lor familial.

Omenirea este în prezent într-o situație de incertitudine asociată cu transformările fundamentale în curs de desfășurare și este însoțită de o serie de amenințări și pericole semnificative pentru aceasta. Una din cele mai importante amenințări este de fapt războiul desfășurat „nu prin căile clasice, ci prin manipularea popoarelor".[17] Acesta este un nou tip de război ce se apropie rapid, cu un spectru întreg de noi tipuri de arme (majoritatea fiind de natură neletală).

Interesul pentru noi tipuri de arme este extrem de mare, deoarece acum, în dimensiunile socio-economice și socio-culturale, există o criză globală a istoriei cauzată de globalizare. Situația actuală în lumea modernă este de așa natură încât moralitatea este cea care acționează ca o resursă strategică pentru supraviețuirea omenirii. În această privință, siguranța societății este de interes ca o problemă filosofică și metodologică, atunci când sunt cercetate natura siguranței societății și condițiile pentru formarea unei teorii complexe a siguranței macrosistemului social. Deoarece acum există o dezvoltare dinamică a societății informaționale și electronico-digitale, problema securității informației devine urgentă. În legătură cu acest proces global, apar o serie de dileme – libertate absolută sau control total, haos sau ordine strictă în politica de rețea etc. –, precum și importanța războaielor informaționale în lumea modernă. Utilizarea ultimelor tehnologii poate reprezenta un pericol pentru societăți și, din acest motiv, cercetătorii acordă atenție locului inteligenței artificiale în sistemul de securitate a informațiilor, perspectivelor sistemelor de comunicații spațiale ca element al armelor genetice, problemelor armelor psihotronice și războiului psihotronic, războaielor în general.

[16] V. Pravdivtsev, *Тайные технологии [Secret technologies]*, Binom. Laboratoriya Znanii, Moscow, 2012, pp. 54-57.
[17] A. Toffler, H. Toffler, *Război și anti-război: supraviețuirea în zorii secolului XXI*, Editura Antet, București, 1995, p. 6.

Operațiile non-cinetice

Apariția de noi instrumente militare și evenimentele politico-militare din ultimul deceniu se combină și produc efecte la nivel tactic, operativ, strategic și chiar politic, fără a se recurge la forța militară clasică. În domeniul militar de exemplu, experiențele din Irak, Afganistan și Siria au produs modificări la nivelul doctrinelor și conceptelor operaționale non-cinetice atât pentru SUA, cât și pentru restul statelor NATO. *Manualul american pentru combaterea insurgenței* și *Manualul pentru operațiuni de stabilizare* al Marii Britanii[18] fac trimiteri la metode de acțiune non-cinetice, cum ar fi operațiuni media, operațiuni de informare (câștigarea încrederii populației), analiza factorului uman din zona de conflict vizată, angajarea liderilor-cheie, analiza rețelelor sociale etc.[19]

Mai mult decât atât, în ultimul deceniu, în cadrul armatelor occidentale s-a adoptat ideea că în majoritatea problemelor de securitate internațională este necesară o abordare multifuncțională ce implică atât activități militare, cât și non-militare. O schimbare în structura societății unui stat fragil nu poate fi realizată decât în momentul în care se pune accent pe o „abordare globală" ce integrează politici economice, ajutor financiar, construcția sau reconstrucția infrastructurii, instituirea unui sistem judiciar corect și crearea de instituții democratice.[20] NATO a „îmbrățișat" aceste noțiuni, iar, în prezent, la nivelul Alianței se acordă o importanță majoră domeniului cibernetic, comunicărilor strategice etc., acest lucru ieșind în evidență nu numai în comunicările oficiale în urma summit-urilor, ci și prin crearea diferitor centre de excelență NATO pentru anumite domenii.

Se poate observa cum grupuri, organizații, state-națiune și chiar persoane pot influența politica la nivel internațional prin utilizarea eficientă a informațiilor, puterea informațională devenind astfel unul din cele mai importante elemente ale puterii. Paradigma puterii s-a schimbat datorită exploziei tehnologice din ultimul deceniu. Un exemplu elocvent al impactului puterii informaționale este dat de răspândirea cu succes a ideilor și valorilor occidentale, cum ar fi statul de drept, democrația, libertatea de exprimare, drepturile omului etc., în țările foste comuniste, rezultând astfel o forță amenințătoare din punctul de vedere al regimurilor dictatoriale.

[18] ***, *Joint Doctrine Publication 3-40 - Security and Stabilisation: The Military Contribution*, Chiefs of Staff, November 2009, URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/792974/archive_doctrine_uk_sy_stab_jdp_3_40.pdf, accesat la 21.11.2020.
[19] ***, *FM 3-24/MCWP 3-33.5 - Insurgencies and Countering Insurgencies*, Headquarters, Department of the Army, May 2014, URL: https://fas.org/irp/doddir/army/fm3-24.pdf, accesat la 21.11.2020.
[20] T.W. Brocades Zaalberg, *Soldiers and Civil Power: Supporting or Substituting Civil Authorities in Modern Peace Operations*, Amsterdam University Press, Amsterdam, 2006.

Deși în mare parte instrumentele non-cinetice sunt aplicate cu succes, folosirea acestora s-a dovedit dificilă în unele cazuri. Nu este o surpriză deoarece, chiar și în aplicarea forței militare clasice, siguranța atingerii rezultatelor dorite nu este garantată. În acest sens, ies în evidență cel puțin patru probleme ce par să afecteze operațiile non-cinetice, mai mult decât cele cinetice:

- asimetria adversarilor ce nu pot fi controlați;
- greșeli ale strategiei aplicate;
- obstacole organizaționale, birocratice și politice;
- deficiențe în înțelegerea afectării schimbărilor comportamentale.[21]

Strategiile non-cinetice au ca scop „epuizarea” țării vizate și implică o gamă largă de acțiuni, precum operații pentru a destabiliza economia, securitatea militară, sfera culturală și filosofică și, bineînțeles, atacuri cibernetice. Statul agresor, fără o declarație oficială de război, atacă structurile guvernamentale, economia, sfera informațională, media, valorile culturale, forțele de ordine și armata regulată a țării vizate. Apoi, la un anumit stadiu, apar ostilitățile prin participarea mercenarilor, companiilor militare private susținute cu personal, arme și finanțe din străinătate.

Pentru a înțelege și mai bine importanța resurselor non-cinetice putem face o scurtă analiză asupra conflictului din Ucraina. Folosind elemente care stau la baza mecanismelor unor operații non-cinetice, Rusia a încercat anterior declanșării conflictului să exercite presiuni economice asupra fostului „satelit”. S-a putut observa la momentul respectiv modul în care Moscova și-a folosit puterea economică împotriva Ucrainei în special în sectorul energetic: încă de la începutul anului 2016, în paralel cu amenințările de întrerupere a aprovizionării cu energie, Rusia a aplicat în mod activ sancțiuni economice. Totodată, a încercat să creeze aparent „interacțiuni” cu țările occidentale și, mai ales, cu Uniunea Europeană, implicându-se activ în așa-numitul „grup de contact Normandia”.[22]

Tot în aceeași perioadă, Rusia a utilizat în mod activ mecanisme de atac cibernetic împotriva statului ucrainean. A urmat apoi dominarea mass-media din Ucraina și a rețelelor sociale, în special prin apariția unei multitudini de știri false. Concomitent, Rusia a acordat sprijin financiar, logistic și umanitar protestatarilor din anumite regiuni ucrainene.

Aceste acțiuni au permis ca două regiuni din estul Ucrainei, Donețk și Lugansk, să se transforme de fapt în state independente cu drepturi depline, în ciuda faptului că respectivele regiuni, spre deosebire de Crimeea, nu au avut niciodată autonomie politică și nici un statut special. Și asta în ciuda faptului că nici măcar un singur stat (nici Rusia) nu a recunoscut oficial autonomia acestor regiuni.

Odată cu apariția amenințărilor de natură nucleară, războiul letal devine un mijloc ineficient în asigurarea dominației unui adversar. Armele nucleare au dus la excluderea câștigătorilor războiului tradițional. Războiul nuclear conduce automat la distrugerea întregii civilizații umane, a cărei dezvoltare este legată de fenomenul războaielor continue. În prezent, limita războaielor tradiționale a fost atinsă, făcându-și apariția războaiele non-cinetice, deoarece, astăzi, excluderea posibilității apariției unui război clasic a devenit sarcina universală a omenirii. Totodată, trebuie să realizăm faptul că umanitatea însăși nu poate opri conflictele de tipul „război rece” și nici pe cele interne. Războaiele continuă, dar sub alte forme, ele fiind informaționale, cibernetice, diplomatice, economice, financiare etc., în contextul în care actorii statali puternici creează continuu forme sofisticate de confruntare non-cinetică și iau decizii în concordanță cu interesele lor naționale și internaționale în distribuirea și redistribuirea resurselor și a influenței globale.[23]

Concluzii

Schimbările din mediul de securitate sunt tot mai evidente, tehnologiile emergente și disruptive se dezvoltă exponențial și generează noi riscuri și amenințări care produc instabilitate, incertitudine și confuzie. În acest context, pe lângă operațiile militare tradiționale, capătă o importanță tot mai mare operațiile desfășurate în mediul informațional și virtual, unde tehnologiile emergente sunt integrate și interconectate. De aceea, am pus accentul pe delimitarea conceptuală a operațiilor informaționale, cibernetice, non-letale și non-cinetice pentru a identifica fizionomia și caracteristicile acestora.

Totodată, apreciem că operațiile non-cinetice îndeplinesc rolul de integrator, iar celelalte tipuri de acțiuni informaționale, cibernetice și non-letale sunt integrate și interconectate în proporții diferite în cadrul acestora. Din acest punct de vedere, considerăm că viitorul aparține tehnologiilor emergente și disruptive de tipul rețelelor 5G, inteligenței artificiale, sistemelor spațiale și de arme autonome, roboticii, mutațiilor genetice etc., care vor genera o multitudine de operații desfășurate în mediul non-cinetic.

În concluzie, pledăm pentru aprofundarea conceptelor de operații informaționale, cibernetice, non-letale și non-cinetice pentru a fi abordate în sistemul de învățământ militar și integrate în cadrul unei strategii operaționale.

[21] P.A.L. Ducheine, F.P.B. Osinga (eds.), *Netherlands Annual Review of Military Studies 2017 - Winning Without Killing: The Strategic and Operational Utility of Non Kinetic Capabilities in Crises*, T.M.C. Asser Press, The Hague, 2017.

[22] ***, *Normandy Format*, Wikipedia, URL : https://en.wikipedia.org/wiki/Normandy_Format, accesat la 23.11.2020.

[23] A.D. Pintili, *Fisionomy of Non-Kinetic Operations in the Context of Armed Conflict*, Proceedings of the 16th International Scientific Conference “Strategies XXI: Global Security and National Defence”, “Carol I” National Defence University, Bucharest, Romania, 25-26 June 2020, pp. 297-301.

Bibliografie:

1. ***, *Directive 3000.03E: DoD Executive Agent for Non-Lethal Weapons (NLW), and NLW Policy*, U.S. Department of Defense, 25 April 2013, URL: http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/300003p.pdf?ver=2018-10-24-112944-467.
2. ***, *FM 3-24/MCWP 3-33.5 - Insurgencies and Countering Insurgencies*, Headquarters, Department of the Army, May 2014, URL: https://fas.org/irp/doddir/army/fm3-24.pdf.
3. ***, *ISO/IEC 27032:2012 – Information technology - Security techniques – Guidelines for cybersecurity*, URL: https://www.iso27001security.com/html/27032.html.
4. ***, *Joint Doctrine Publication 3-40 - Security and Stabilisation: The Military Contribution*, Chiefs of Staff, November 2009, URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/792974/archive_doctrine_uk_sy_stab_jdp_3_40.pdf.
5. ***, *Joint Publication 3-13.1. - Electronic Warfare*, US Joint Chiefs of Staff, 2007.
6. ***, *Кибервойны (Cyberwarfare)*, Anti-Malware, URL: https://www.anti-malware.ru/threats/cyberwarfare.
7. ***, *Non-Lethal Weapons and Future Peace Enforcement Operations*, RTO Techical Report TR-SAS-040, NATO, November 2004.
8. ***, *Normandy Format*, Wikipedia, URL : https://en.wikipedia.org/wiki/Normandy_Format.
9. Baranov V.N., V.V. Lazarev, V.V. Selivanov, *Preconditions and capabilities of development and deployment of special means of combined non-lethal effect*, Proceedings of the 3rd European Symposium on Non-Lethal Weapons, Ettlingen, Germany, 10-12 May 2005.
10. Brocades Zaalberg T.W., *Soldiers and Civil Power: Supporting or Substituting Civil Authorities in Modern Peace Operations*, Amsterdam University Press, Amsterdam, 2006.
11. Cartwright M., „Odysseus”, *Ancient History Encyclopedia*, 31 December 2012, URL: https://www.ancient.eu/odysseus.
12. Danilov N.V., *Компьютерные технологии как оружие информационно-психологического действия [Computer technologies as a weapon of information and psychological action]*, Proceedings of „The Information Security of Russia” Conference, Moscow, 1998.
13. Ducheine P.A.L., F.P.B. Osinga (eds.), *Netherlands Annual Review of Military Studies 2017 - Winning Without Killing: The Strategic and Operational Utility of Non Kinetic Capabilities in Crises*, T.M.C. Asser Press, The Hague, 2017.
14. Nye J.S., Jr., *Viitorul puterii*, Editura Polirom, Iași, 2012.
15. Pintili A.D., *Fisionomy of Non-Kinetic Operations in the Context of Armed Conflict*, Proceedings of the 16th International Scientific Conference “Strategies XXI: Global Security and National Defence”, “Carol I” National Defence University, Bucharest, Romania, 25-26 June 2020.
16. Polikarpov V.S., E.V. Polikarpova, *Войны будущего [The wars of the future]*, Algoritm Publishing House, Moscow, 2015.
17. Pravdivtsev V., *Тайные технологии [Secret technologies]*, Binom. Laboratoriya Znanii, Moscow, 2012.
18. Samsonov S., „Как воспринимаются запахи [How odors are perceived]”, *Наука и жизнь [“Science and Life” Journal]*, No. 4, 1988.
19. Selivanov V.V., D.P. Levin, *Non-lethal weapon role and place in complex security systems*, Proceedings of the 7th European Symposium on Non-Lethal Weapons, Ettlingen, Germany, 3-5 June 2013.
20. Sidorin A.N., V.M. Prishchepov, V.P. Akulenko, *Vooruzhennye sily USA v XXI veke: Voenno-teoreticheskii trud [The U.S. Armed Forces in the XXI Century]*, Progress Publishers, Moscow, 2013.
21. Sokolov V.N., *Оружие будущего. Тайны новейших военных разработок [Weapons of the Future: Secrets of the Latest Military Development]*, Literature Publishing House, Minsk, 1998.
22. Toffler A., H. Toffler, *Război și anti-război: supraviețuirea în zorii secolului XXI*, Editura Antet, București, 1995.
23. Zhukov V., „Взгляды военного руководства США на ведение информационной войны [The views of the US military leadership on information warfare]”, *Зарубежное военное обозрение [Foreign Military Review]*, No. 1, 2001, URL: http://pentagonus.ru/publ/22-1-0-175.

Colocviu strategic
Redactor: CS II dr. Cristian BĂHNĂREANU
Pagină web: https://cssas.unap.ro/ro/cs.htm
e-ISSN 1842-8096, 81/2021

Centrul de Studii Strategice de Apărare și Securitate
Adresă: șos. Panduri, nr. 68-72, sector 5, București
Telefon: 021.319.56.49, Fax: 021.319.57.80
E-mail: cssas@unap.ro, Website: https://cssas.unap.ro